CHAPITRE 7
STRUCTURES ALGÉBRIQUES

⊙ C'est par l'intermédiaire de la résolution des équations polynomiales par radicaux qu'est intervenue pour la première fois la structure de **groupe** : c'est GALOIS (Évariste GALOIS : mathématicien français 1811-1832) qui l'a introduit à propos des permutations des racines de telles équations. ABEL (Niels ABEL : mathématicien norvégien 1802-1829), comme GAUSS et LAGRANGE avaient déjà montré la voie à propos de ces équations sans découvrir la structure appropriée. Grâce aux travaux de GALOIS, on aboutit à l'impossibilité de la résolution par radicaux pour les équations polynomiales de degré supérieur ou égal à 5.

⊙ Dès lors, l'algèbre moderne entame un parcours fécond : BOOLE (Georges BOOLE : logicien, mathématicien et philosophe britannique 1815-1864) crée l'**algèbre** qui porte son nom pour modéliser la logique, HAMILTON (Sir William Rowan HAMILTON : mathématicien, physicien et astronome irlandais 1805-1865) invente les **quaternions**. Parallèlement, KUMMER (Ernst KUMMER : mathématicien allemand 1810-1893) généralise les structures galoisiennes et étudie les structures de **corps** et d'**anneau** ; DEDEKIND (Richard DEDEKIND : mathématicien allemand 1831-1916) définit les **idéaux** (déjà entrevus par KUMMER et GAUSS) qui permettront de généraliser et reformuler les grands théorèmes d'arithmétique.

PARTIE 7.1 : LOIS DE COMPOSITION INTERNES

7.1.1 : Définition d'une loi de composition interne

Définition 7.1

Soit E *un ensemble non vide, on appelle* **loi de composition interne** *(en abrégé* **lci***) toute application de* $E \times E$ *dans* E*, notée par exemple* $*$ *mais on notera* $x * y$ *l'image du couple* $(x, y) \in E^2$.

EXEMPLE 7.1 :

- Dans l'ensemble $E = \mathbb{N}^*$ on dispose des lois $+$, $\times$, $\mathtt{pgcd}$, $\mathtt{ppcm}$.
- Dans l'ensemble $E = \mathbb{R}$ on dispose des lois $+$, $\times$, $\mathtt{Min}$, $\mathtt{Max}$, $-$.
- Si E est un ensemble, on dispose dans $\mathcal{P}(E)$ des lois $\cap$, $\cup$, Δ, $\setminus$.
- Si E est un ensemble non vide, on a dans $\mathcal{F}(E, E)$ la loi composition $\circ$.

7.1.2 : Caractéristiques de la loi

Définition 7.2

Soit E *un ensemble non vide muni de deux lcis* $*$ *et* $\top$*, on dit que :*

- $*$ *est* **commutative** *si* $\forall (x, y) \in E^2,\ x * y = y * x$.
- $*$ *est* **associative** *si* $\forall (x, y, z) \in E^3,\ x * (y * z) = (x * y) * z$.
- $*$ *est* **distributive par rapport à** $\top$ *si* $\forall (x, y, z) \in E^3$,
$$x * (y \top z) = (x * y) \top (x * z) \text{ et } (y \top z) * x = (y * x) \top (z * x).$$

REMARQUE 7.1 :

- *Si une loi* $*$ *est associative et commutative, cela nous permet de définir le "produit" de* n *éléments de* E *sans avoir à se préoccuper de l'ordre des termes ni du parenthésage. Cela justifie dans ce cas les notations* $\sum_{k=1}^{n} x_k$ *si la loi est la loi* $+$, $\prod_{k=1}^{n} x_k$ *si la loi est la loi* $\times$, $\bigcap_{k=1}^{n} A_k$ *si la loi est la loi* $\cap$, *etc....*

• *Le nombre de parenthésages possibles d'un produit de n termes (dans un ensemble muni d'une lci quelconque) est noté C_n et est appelé le n-ième nombre de* CATALAN *(Eugène Charles* CATALAN *: mathématicien franco-belge, spécialisé en théorie des nombres 1814-1894) : on a par convention $C_0 = 0$, $C_1 = 1$, bien sûr $C_2 = 1$ et $C_3 = 2$ et par calcul $C_4 = 5$, $C_5 = 14$, etc... .*

EXEMPLE 7.2 :
- $\setminus$ n'est ni commutative ni associative.
- $\cap$ est distributive par rapport à Δ (mais pas l'inverse).
- $\circ$ n'est pas distributive par rapport à $+$.
- Max est distributive par rapport à Min dans $\mathbb{R}$ et vice-versa.

7.1.3 : Caractéristiques des éléments

Définition 7.3

Soit E un ensemble muni d'une lci $*$ et $e \in E$, on dit que :
- *e est* **neutre à gauche** *si $\forall x \in E,\ e * x = x$.*
- *e est* **neutre à droite** *si $\forall x \in E,\ x * e = x$.*
- *e est* **neutre** *s'il l'est à gauche et à droite.*

EXEMPLE 7.3 :
- 0 est neutre pour $+$ dans les ensembles $\mathbb{N}$, $\mathbb{Z}$, $\mathbb{Q}$, $\mathbb{R}$, $\mathbb{C}$.
- E est neutre pour $\cap$ dans $\mathcal{P}(E)$ et $\emptyset$ est neutre pour $\cup$ et Δ dans $\mathcal{P}(E)$.
- $\emptyset$ est neutre à droite pour $\setminus$ dans $\mathcal{P}(E)$ mais pas neutre à gauche.

Proposition 7.1

On se place dans un ensemble E muni d'une lci $*$:
- **Si e_1 est neutre à gauche et e_2 est neutre à droite alors $e_1 = e_2$.**
- **Si E possède un neutre alors celui-ci est unique.**

REMARQUE 7.2 :
- *Si la loi $*$ est associative dans E et possède un neutre e, si $x \in E$ et $n \in \mathbb{N}$ on définit sans ambiguïté x^n en convenant que $x^0 = e$, que $x^1 = x$ et que $\forall n \in \mathbb{N},\ x^{n+1} = x^n * x$, on a alors $x^{n+1} = x * x^n$.*
- *Si la loi est la loi $+$ alors on écrit nx à la place de x^n.*
- *Si x et y sont deux éléments de E et qu'on a $x * y = y * x$ alors : $\forall n \in \mathbb{N},\ (x * y)^n = x^n * y^n$.*

Définition 7.4

Soit E un ensemble muni d'une lci $*$, d'un neutre e. Soit $x \in E$, on dit que :
- *x est* **inversible à gauche** *si $\exists y \in E,\ y * x = e$.*
- *x est* **inversible à droite** *si $\exists y \in E,\ x * y = e$.*
- *x est* **inversible** *si $\exists y \in E,\ x * y = y * x = e$.*

EXEMPLE 7.4 : Soit $f \in \mathcal{F}(E, E)$, alors f est inversible à droite (pour la loi $\circ$) ssi f est surjective.

REMARQUE 7.3 :
- *Attention, il est possible que x soit inversible à gauche et à droite sans être inversible.*
- *Avec ces hypothèses et si la loi $*$ est associative, si on suppose x inversible à gauche et à droite, alors il existe un unique élément y dans E tel que $x * y = y * x = e$. Ce qui nous permet de poser :*

Définition 7.5

Soit E un ensemble muni d'une lci $*$ associative, d'un neutre e et soit $x \in E$ inversible alors on appelle **inverse** *de x (ou* **opposé** *si la loi est la loi $+$) note x^{-1} (ou $-x$ si la loi est la loi $+$) l'unique élément tel que $x^{-1} * x = x * x^{-1} = e$ (ou $x + (-x) = (-x) + x = e$ si la loi est la loi $+$).*

REMARQUE 7.4 : e est toujours inversible et est son propre inverse car $e * e = e$.

EXEMPLE 7.5 :

- Dans $\mathcal{P}(E)$ muni de la loi $\cup$ le seul inversible est $\emptyset$ (c'est-à-dire le neutre justement).
- Dans $\mathcal{P}(E)$ muni de la loi Δ toute partie A est inversible et est son propre inverse.
- Si $f \in \mathcal{F}(E, E)$ muni de la loi $\circ$, dire que f est inversible c'est affirmer l'existence de $g \in \mathcal{F}(E, E)$ telle que $f \circ g = g \circ f = id_E$. Ainsi : ($f$ inversible) $\iff$ (f bijective) (son inverse est sa réciproque).

Proposition 7.2

Soit E un ensemble non vide muni d'une loi $*$ associative et d'un neutre e, deux éléments x et y inversibles de E, alors x^{-1} et $x * y$ sont inversibles et : $(x^{-1})^{-1} = x$ et $(x * y)^{-1} = y^{-1} * x^{-1}$.

REMARQUE 7.5 :

- *Si x est inversible pour une loi $*$ associative dans E alors on définit, si $n \in \mathbb{N}^*$: $x^{-n} = (x^{-1})^n$.*
- *Quelques calculs simples permettent d'établir que : $\forall (n, m) \in \mathbb{Z}^2,\ x^{n+m} = x^n * x^m$, $(x^n)^{-1} = x^{-n}$.*
- *Si, de plus, les deux éléments x et y de E sont inversibles et qu'en plus ils commutent ($x * y = y * x$) alors on a même les relations ; $\forall n \in \mathbb{Z},\ (x * y)^n = x^n * y^n$.*

Définition 7.6

Soit E un ensemble non vide muni d'une loi $*$ et $a \in E$, on dit que a est :

- **régulier à gauche** *si* $\forall (x, y) \in E^2,\ a * x = a * y \Longrightarrow x = y$.
- **régulier à droite** *si* $\forall (x, y) \in E^2,\ x * a = y * a \Longrightarrow x = y$.
- **régulier** *si a l'est à gauche et à droite.*

REMARQUE 7.6 : Dire que a est régulier à gauche, c'est dire que $g_a : E \to E$ est injective où g_a est définie par : $\forall x \in E,\ g_a(x) = a * x$.

EXEMPLE 7.6 : • Dans $\mathbb{Z}$ muni de la loi $\times$, 3 est régulier mais pas inversible.

- Dans $\mathcal{P}(E)$ muni de la loi $\cup$, seul $\emptyset$ est régulier et il est aussi inversible puisque c'est le neutre.
- Dans $\mathcal{F}(E, E)$ muni de la loi $\circ$: (f est régulière à gauche) $\iff$ (f est injective).

Proposition 7.3

Si $a \in E$ où E est un ensemble non vide muni d'une loi $*$ associative possédant un neutre e :

- **a inversible à gauche $\Longrightarrow$ a régulier à gauche.**
- **a inversible à droite $\Longrightarrow$ a régulier à droite.**
- **a inversible $\Longrightarrow$ a régulier.**

REMARQUE 7.7 : Les réciproques de ces implications sont fausses en général.

EXEMPLE 7.7 :

- Par exemple 3 est régulier dans $\mathbb{Z}$ alors qu'il n'y est pas inversible.
- Les fonctions injectives sont régulières à gauche pour la loi $\circ$ dans $\mathcal{F}(E, E)$ mais ne sont pas inversibles en général car une application injective n'est pas forcément bijective.

Définition 7.7

Soit E un ensemble non vide muni d'une loi $*$ et $a \in E$, on dit que :

- **absorbant à gauche** *si* $\forall x \in E,\ a * x = a$.
- **absorbant à droite** *si* $\forall x \in E,\ x * a = a$.
- **absorbant** *si a l'est à gauche et à droite.*

EXEMPLE 7.8 : • $\emptyset$ est absorbant pour la loi $\cap$ dans $\mathcal{P}(E)$.

- 1 est absorbant à gauche pour la loi "exponentiation" dans $\mathbb{N}^*$.
- 1 est absorbant pour la loi pgcd dans $\mathbb{N}^*$.

7.1.4 : Caractéristiques de l'ensemble

Définition 7.8

Soit E *muni d'un loi* $*$ *et* A *une partie de* E*, on dit que* A *est* **stable** *par* $*$ *si* $\forall (x,y) \in A^2,\ x * y \in A$.

EXEMPLE 7.9 :

- Les entiers pairs (resp. impairs) sont stables dans $\mathbb{Z}$ muni de la loi $\times$. Par contre les entiers pairs (et seulement eux) sont stables dans $\mathbb{Z}$ pour la loi $+$.
- Les translations sont stables dans l'ensemble des transformations du plan muni de la loi $\circ$.
- $]-1;1[$ est stable dans $\mathbb{R}$ muni de la loi $\times$.

REMARQUE 7.8 : Si A *est stable dans* E*, alors* A *est muni de la loi de composition interne* $*_A$ *induite par* $*$ *dans* A*, qui est définie par :* $\forall (x,y) \in A^2,\ x *_A y = x * y$*. Celle-ci est commutative si* $*$ *l'est, associative si* $*$ *l'est, mais n'admet par forcément de neutre (même si* E *en admet un), par contre elle peut avoir des propriétés que* $*$ *n'a pas.*

Définition 7.9

Avec ces notations, A *est dit* **absorbant** *si* $\forall a \in A, \forall x \in E,\ x * a \in A$ *et* $a * x \in A$.

EXEMPLE 7.10 : • Les entiers pairs sont absorbants dans $\mathbb{Z}$ muni de la loi $\times$.

- Si $A \subset E$ alors $\mathcal{P}(A)$ est absorbant dans $\mathcal{P}(E)$ muni de la loi $\cap$.

PARTIE 7.2 : GROUPES

7.2.1 : Définition d'un groupe et exemples

Définition 7.10

Soit G *un ensemble non vide muni d'une loi de composition interne* $*$*, on dit que* $(G,*)$ *est un* **groupe** *si la loi* $*$ *est associative, s'il existe un neutre* e *dans* G *pour la loi* $*$ *et si tous les éléments de* G *possèdent un inverse.*

Si la loi $*$ *est de plus commutative, on dira que le groupe est* **abélien** *ou* **commutatif**.

REMARQUE 7.9 : On constate et on s'en servira extrêmement souvent : dans un groupe tout élément est régulier car il est inversible.

EXEMPLE 7.11 : • $(\mathbb{Z},+)$, $(\mathbb{R},+)$ etc... sont des groupes abéliens de neutre 0.

- $(\mathbb{Q}^*,\times)$, $(\mathbb{C}^*,\times)$ sont des groupes abéliens de neutre 1.
- L'ensemble des translations du plan est un groupe de neutre id_E pour la loi $\circ$.
- $(\mathcal{P}(E),\Delta)$ est un groupe abélien de neutre $\emptyset$.
- On peut définir le groupe des isométries du plan qui laissent globalement un objet géométrique invariant : par exemple le groupe du triangle équilatéral a 6 éléments, le groupe du carré en a 8, le groupe du losange en a 4.

REMARQUE 7.10 : Pour un entier $n \in \mathbb{N}^*$*, on note* $\boldsymbol{\sigma}_n$ *le* **groupe symétrique** *: c'est-à-dire l'ensemble de toutes les permutations de* $[\![1;n]\!]$*. Il y a bien sûr* $n!$ *telles bijections de* $[\![1;n]\!]$ *dans* $[\![1;n]\!]$ *et la loi interne dans cet ensemble est* $\circ$ *qui conserve la notion de bijection et les ensembles de départ et d'arrivée.*

EXEMPLE 7.12 : Les éléments de ce groupe peuvent être notés $\sigma = \begin{pmatrix} 1 & 2 & 3 & 4 \\ 4 & 2 & 1 & 3 \end{pmatrix}$; σ est ainsi l'application qui va de $[\![1;4]\!]$ dans lui-même et qui vérifie $\sigma(1)=4$, $\sigma(2)=2$, $\sigma(3)=1$ et $\sigma(4)=3$.

REMARQUE 7.11 : Ce groupe n'est pas abélien dès que $n \geqslant 3$ *car si on pose* $\sigma_1 = \begin{pmatrix} 1 & 2 & 3 & \cdots \\ 2 & 1 & 3 & \cdots \end{pmatrix}$ *et* $\sigma_2 = \begin{pmatrix} 1 & 2 & 3 & \cdots \\ 1 & 3 & 2 & \cdots \end{pmatrix}$, *alors* $\begin{pmatrix} 1 & 2 & 3 & \cdots \\ 2 & 3 & 1 & \cdots \end{pmatrix} = \sigma_1 \circ \sigma_2 \neq \sigma_2 \circ \sigma_1 = \begin{pmatrix} 1 & 2 & 3 & \cdots \\ 3 & 1 & 2 & \cdots \end{pmatrix}$.

Définition 7.11

Si $(G, *)$ *est un groupe fini et que* $G = \{x_1, x_2, \cdots, x_n\}$ *alors on peut voir la loi* $*$ *dans* G *en considérant un tableau ayant* n *lignes et* n *colonnes et qui contient dans la ligne* i *et la colonne* j *le produit* $x_i * x_j$. *Ce tableau s'appelle la* **table de la loi**.

EXEMPLE 7.13 :

Si on note K le groupe du losange aussi appelé groupe de KLEIN (Félix KLEIN : mathématicien allemand 1849-1925), alors $K = \{f_1, f_2, f_3, f_4\}$ où f_1 est l'identité, f_2 la symétrie centrale de centre O le centre du losange, f_3 la réflexion d'axe une des deux diagonales du losange et f_4 la réflexion par rapport à l'autre diagonale. Ainsi on obtient la table suivante (à droite) de la loi $\circ$ dans le groupe K. On a aussi (à gauche) la table de $\mathbb{U}_4 = \{\omega_1, \omega_2, \omega_3, \omega_4\}$ où $\omega_1 = 1$, $\omega_2 = i$, $\omega_3 = -1$ et $\omega_4 = -i$.

$\times$	ω_1	ω_2	ω_3	ω_4
ω_1	ω_1	ω_2	ω_3	ω_4
ω_2	ω_2	ω_3	ω_4	ω_1
ω_3	ω_3	ω_4	ω_1	ω_2
ω_4	ω_4	ω_1	ω_2	ω_3

$\circ$	f_1	f_2	f_3	f_4
f_1	f_1	f_2	f_3	f_4
f_2	f_2	f_1	f_4	f_3
f_3	f_3	f_4	f_1	f_2
f_4	f_4	f_3	f_2	f_1

REMARQUE 7.12 : On constate que dans chaque ligne et dans chaque colonne, on retrouve une fois et une seule chaque élément du groupe : ceci se montre facilement en considérant les applications $g_a : G \to G$ *définie par :* $\forall x \in G,\ g_a(x) = a * x$ *et* $d_a : G \to G$ *définie par :* $\forall x \in G,\ d_a(x) = x * a$.

En effet ces applications sont bijectives car $g_a \circ g_{a^{-1}} = id_G$ *et* $d_a \circ d_{a^{-1}} = id_G$.

REMARQUE 7.13 : Si $(G_1, *_1)$ *et* $(G_2, *_2)$ *sont deux groupes (de neutres respectifs* e_1 *et* e_2*) alors on munit* $G = G_1 \times G_2$ *de la loi* $*$ *définie par :* $\forall (x_1, y_1, x_2, y_2) \in G_1^2 \times G_2^2,\ (x_1, x_2) * (y_1, y_2) = (x_1 *_1 y_1, x_2 *_2 y_2)$. *Alors* $e = (e_1, e_2)$ *est neutre pour* $*$ *dans* G, $*$ *est associative et tout élément* $(x_1, x_2) \in G$ *admet pour inverse* (x_1^{-1}, x_2^{-1}) *donc* $(G, *)$ *est un groupe, appelé* **groupe produit**.

7.2.2 : Sous-groupes et engendrement

Définition 7.12

Soit $(G, *)$ *un groupe de neutre* e *et* $H \subset G$.
On dit que H *est un* **sous-groupe** *de* G *si* $e \in H$, *si* H *est stable par* $*$ *et si :* $\forall x \in H,\ x^{-1} \in H$.

REMARQUE 7.14 :

- *Avec ces notations,* $(H, *_H)$ *est un groupe car la loi* $*_H$ *induite par* $*$ *dans* H *est associative, possède un neutre* e, *et tous les éléments de* H *sont inversibles pour* $*_H$ *(l'inverse de* $x \in H$ *dans* H *est* x^{-1}*).*
- $\{e\}$ *est toujours un sous-groupe de* G, *comme l'est* G *en entier.*

EXEMPLE 7.14 : • $\mathbb{Q}$ est un sous-groupe de $\mathbb{R}$ pour la loi $+$.
- $\mathbb{R}_+^*$ est un sous-groupe de $\mathbb{C}^*$ pour la loi $\times$.
- Si $A \subset E$, $\mathcal{P}(A)$ est un sous-groupe de $\mathcal{P}(E)$ pour la loi Δ.

Proposition 7.4

Avec les mêmes notations que ci-dessus, on a l'équivalence entre :

(i) H **est un sous-groupe de** G.

(ii) $H \neq \emptyset$ **et** $\forall (x, y) \in H^2,\ x * y^{-1} \in H$.

REMARQUE 7.15 : Si la loi est la loi $+$, cette condition (ii) *devient* $H \neq \emptyset$ *et* $\forall (x,y) \in H^2,\ x - y \in H$.

Méthode

Soit $(G,*)$ **un groupe et** $H \subset G$**. Pour montrer que** H **est un sous-groupe de** G **:**
- **on montre tout d'abord que** $e \in H$ **(c'est souvent plus simple),**
- **on se donne** $(x,y) \in H^2$ **et on montre que** $x * y^{-1} \in H$ **(ou** $x - y \in H$ **si la loi est** $+$**).**

Proposition 7.5

Si G **est un groupe et** $(H_i)_{i\in I}$ **une famille de sous-groupes de** G **alors l'intersection** $\bigcap_{i\in I} H_i$ **est aussi un sous-groupe de** G**.**

Proposition 7.6

Soit $(G,*)$ **un groupe et** $A \subset G$**, l'intersection de tous les sous-groupes de** G **contenant** A **est un sous-groupe de** G **contenant** A **: c'est le plus petit parmi les sous-groupes contenant** A**.**

Définition 7.13

Avec ces notations, on note $< A >$ *ce sous-groupe et on l'appelle le* **sous-groupe engendré** *par* A*.*

Méthode

Pour montrer que $H = < A >$**, il suffit de montrer que :**
- H **est un sous-groupe de** G**,**
- $A \subset H$**,**
- ($A \subset K$ **et** K **sous-groupe de** G) $\Longrightarrow H \subset K$**.**

EXEMPLE 7.15 : Dans le groupe D_4 (groupe diédral d'ordre 4 à 8 éléments), le sous-groupe engendré par la rotation d'angle $\frac{\pi}{2}$ possède 4 éléments.

REMARQUE 7.16 : Plus généralement, si $x_0 \in G$*, alors l'ensemble des puissances de* x_0*, c'est-à-dire* $H = \{x_0^n \mid n \in \mathbb{Z}\}$*, est le sous-groupe engendré par le singleton* $\{x_0\}$*.*

Définition 7.14

Un groupe engendré par un seul de ses éléments est dit **monogène** *s'il est infini et* **cyclique** *s'il est fini.*

7.2.3 : Morphisme de groupes

Définition 7.15

Soit $(G,*)$ *et* $(G',*')$ *deux groupes et* $f : G \to G'$ *une application, on dit que* f *est un* **morphisme** *de groupes si :* $\forall (x,y) \in G^2,\ f(x*y) = f(x) *' f(y)$.

EXEMPLE 7.16 :
- Si x_0 est un élément d'un groupe G alors l'application $f : \mathbb{Z} \to G$ définie par : $\forall n \in \mathbb{Z},\ f(n) = x_0^n$ est un morphisme de $(\mathbb{Z},+)$ dans $(G,*)$.
- L'application $f : \mathbb{U}_8 \to \mathbb{U}_4$ définie par : $\forall z \in \mathbb{U}_8,\ f(z) = z^2$ est un morphisme de groupes .
- L'exponentielle est un morphisme de $(\mathbb{R},+)$ dans $(\mathbb{R}^*,\times)$.

Proposition 7.7

Soit $f : G \to G'$ **un morphisme de groupes, alors si** e **est le neutre dans** G **et** e' **celui dans** G' **:** $f(e) = e'$ **et** $\forall x \in G,\ \forall n \in \mathbb{Z},\ f(x^n) = f(x)^n$ **; en particulier** $f(x^{-1}) = \big(f(x)\big)^{-1}$**.**

Définition 7.16

Soit $f : G \to G'$ *un morphisme alors on dit que :*
- f *est un* **endomorphisme** *si* $G = G'$ *(en tant que groupe).*
- f *est un* **isomorphisme** *si* f *est bijective.*
- f *est un* **automorphisme** *si* $G = G'$ *(en tant que groupe) et* f *bijective.*

EXEMPLE 7.17 : • $x \mapsto x^3$ est un automorphisme de $(\mathbb{R}^*, \times)$.
- $n \mapsto 3n$ est un endomorphisme de $(\mathbb{Z}, +)$.
- Le logarithme népérien est un isomorphisme de $(\mathbb{R}_+^*, \times)$ dans $(\mathbb{R}, +)$.

Proposition 7.8

Soit $f : G \to G'$ **et** $g : G' \to G''$ **deux morphismes de groupes alors** $g \circ f$ **est un morphisme de groupes. De plus, Si** f **est un isomorphisme, alors** $f^{-1} : G' \to G$ **en est aussi un.**

REMARQUE 7.17 :
- *Comme la composée de deux bijections est une bijection, on peut donc affirmer grâce à ce qui précède que la composée de deux isomorphismes en est encore un, la composée de deux endomorphismes en est encore un et que la composée de deux automorphismes en est encore un.*
- *Ce qui implique par exemple que* $\big(\mathrm{Aut}(G), \circ\big)$ *est un groupe, celui-ci est en général non abélien.*

Proposition 7.9

Soit $f : G \to G'$ **un morphisme de groupes,** H **un sous-groupe de** G**,** H' **un sous-groupe de** G'**, alors** $\widehat{f}(H)$ **est un sous-groupe de** G' **et** $f^{<-1>}(H')$ **est un sous-groupe de** G**.**

Définition 7.17

Soit $f : G \to G'$ *un morphisme ; on appelle* **noyau** *de* f*, noté* $\mathrm{Ker}(f)$ *la partie* $\mathrm{Ker}(f) = f^{<-1>}(\{e'\})$ *de* G *; on appelle* **image** *de* f*, notée* $\mathrm{Im}(f)$*, la partie* $\widehat{f}(G)$ *de* G'*.*

REMARQUE 7.18 : $\mathrm{Ker}(f)$ *est un sous-groupe de* G *et* $\mathrm{Im}\, f$ *est un sous-groupe de* G'*.*

EXEMPLE 7.18 : • Si $f = \exp : \mathbb{R} \to \mathbb{R}^*$ alors $\mathrm{Ker}(f) = \{0\}$ et $\mathrm{Im}(f) = \mathbb{R}_+^*$.
- Si $f : x \mapsto x^2$ est l'endomorphisme de $(\mathbb{R}^*, \times)$ alors $\mathrm{Ker}(f) = \{-1, 1\}$ et $\mathrm{Im}(f) = \mathbb{R}_+^*$.
- Si $f : \mathbb{U}_{100} \to \mathbb{U}_{100}$ vérifie : $\forall z \in \mathbb{U}_{100},\ f(z) = z^6$, calculons $f^{<-1>}(\mathbb{U}_{20})$, $\widehat{f}(\mathbb{U}_5)$, $\mathrm{Im}(f)$ et $\mathrm{Ker}(f)$.

Théorème 7.1

Pour un morphisme de groupes $f : G \to G'$**, on a les équivalences :**
- f **injective** $\iff \mathrm{Ker}(f) = \{e\}$**.**
- f **surjective** $\iff \mathrm{Im}(f) = G'$**.**

Méthode

Pour un morphisme de groupes $f : G \to G'$**, on dispose des équivalences suivantes :**
- (f **est surjective**) $\iff \big(\forall y \in G',\ \exists x \in G,\ y = f(x)\big)$**.**
- (f **est injective**) $\iff \big(\forall x \in G,\ f(x) = e' \Longrightarrow x = e\big)$**.**

*REMARQUE 7.19 : (HP) L'***ordre** *d'un élément* x *d'un groupe* G *est* $\begin{cases} p = \infty \ \text{ si } \ \forall n \in \mathbb{N}^*,\ x^n \neq e, \\ p = \mathrm{Min}(n \in \mathbb{N}^*,\ x^n = e) \ \text{ sinon.} \end{cases}$

Si x *est d'ordre fini* p*, on montre avec la division euclidienne que* $< x >= \{e, x, \cdots, x^{p-1}\}$ *(de cardinal* p*). Si de plus le groupe* G *est fini, comme le* **théorème de** LAGRANGE *annonce que la cardinal de tout sous-groupe divise le cardinal du groupe alors* p *divise* $\mathrm{card}\,(G)$*.*

Dans un groupe fini, tout élément est d'ordre fini et cet ordre divise le cardinal du groupe.

PARTIE 7.3 : ANNEAUX ET CORPS

7.3.1 : Définition et exemples

Définition 7.18

Soit A *un ensemble non vide muni de deux lcis* $\top$ *et* $*$*. On dit que* $(A, \top, *)$ *est un* **anneau** *si :*
- $(A, \top)$ *est un groupe commutatif de neutre* 0_A*.*
- $*$ *est associative et distributive par rapport à* $\top$*.*
- *Il existe un neutre* $1_A \neq 0_A$ *pour la loi* $*$ *dans* A*.*

De plus, si la loi $*$ *est commutative, on dira que* A *est un* **anneau commutatif***.*

On dit que l'anneau A *est* **intègre** *si :* $\forall (x, y) \in A^2,\ x * y = 0_A \Longrightarrow x = 0_A$ *ou* $y = 0_A$*.*

EXEMPLE 7.19 : • $(\mathbb{Z}, +, \times)$ est un anneau commutatif intègre, comme $(\mathbb{Q}, +, \times)$, etc... .
- $\big(\mathcal{P}(E), \Delta, \cap\big)$ est un anneau commutatif mais non intègre.
- $\big(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \times\big)$ est aussi un anneau commutatif encore non intègre.
- Par contre, $\big(\mathcal{F}(\mathbb{R}, \mathbb{R}), +, \circ\big)$ n'en est pas un car $\circ$ n'est pas distributive par rapport à $+$.

Définition 7.19

Avec ces notations, si a *est un élément de l'anneau* A*, on dit que :*
- a *est un* **diviseur de zéro** *si :* $a \neq 0_A$ *et* $\exists b \in A,\ b \neq 0_A$ *et* $a * b = 0_A$ *ou* $b * a = 0_A$*.*
- a *est un* **absorbant** *si* $\forall b \in A,\ a * b = b * a = a$*.*
- a *est* **nilpotent** *si :* $\exists n \in \mathbb{N},\ a^n = 0_A$ *(puissance pour la loi* $*$*).*
- a *est* **idempotent** *si* $a * a = a$*.*
- a *est* **involutif** *si* $a * a = 1_A$*.*

REMARQUE 7.20 : Un anneau intègre est un anneau qui ne possède aucun diviseur de zéro.

Proposition 7.10

Soit $(A, +, \times)$ **un anneau de neutre** 0_A **pour la loi** $+$ **et** $(x, y) \in A^2$ **:**
- $x \times 0_A = 0_A \times x = 0_A$ **(0_A est absorbant).**
- $(-x) \times y = x \times (-y) = -(x \times y)$**.**

Proposition 7.11

Si $(x, y) \in A^2$ **vérifie** $xy = yx$ **(on ne note plus la loi** $\times$**), alors on dispose des formules :**
- $\forall n \in \mathbb{N}^*,\ (x+y)^n = \sum_{k=0}^{n} \binom{n}{k} x^k y^{n-k}$ **(binôme de Newton).**
- $\forall n \in \mathbb{N}^*,\ x^n - y^n = (x-y)\left(\sum_{k=0}^{n-1} x^{n-1-k} y^k\right)$ **(sommes des termes d'une suite géométrique).**
- $\forall n \in \mathbb{N},\ x^{2n+1} + y^{2n+1} = (x+y)\left(\sum_{k=0}^{2n} (-1)^k x^{2n-k} y^k\right)$**.**

7.3.2 : Les éléments inversibles d'un anneau

Définition 7.20

Dans un anneau A *et pour* $x \in A$*, on dit que* x *est* **inversible** *s'il existe* $y \in A$ *tel que* $xy = yx = 1_A$*. On note alors* x^{-1} *cet inverse comme il se doit.*

EXEMPLE 7.20 :

- Dans $\mathbb{Z}$, les seuls inversibles sont 1 et -1 et sont bien sûr leur propre inverse.
- Dans $\mathcal{F}(\mathbb{R}, \mathbb{R})$ les fonctions inversibles sont les fonctions qui ne s'annulent pas sur $\mathbb{R}$ (comme ch).

Théorème 7.2

Soit A un anneau et $A^\times$ l'ensemble des inversibles de A, on a : $(A^\times, \times)$ est un groupe.

EXEMPLE 7.21 : $\mathbb{Z}^\times = \{-1, 1\}$ et $\mathbb{Q}^\times = \mathbb{Q}^*$.

7.3.3 : Sous-anneau et morphismes d'anneaux

Définition 7.21

Soit A un anneau et $B \subset A$, on dit que B est un **sous-anneau** *de A si B est un sous-groupe de A pour la loi $+$, si $1_A \in B$ et si B est stable pour la loi $\times$.*

Méthode

Soit A un anneau et $B \subset A$, B est un sous-anneau de A si et seulement si on a :

- $1_A \in B$,
- $\forall (x, y) \in B^2,\ x - y \in B$,
- $\forall (x, y) \in B^2,\ x \times y \in B$.

EXEMPLE 7.22 : • Le seul sous-anneau de $\mathbb{Z}$ est $\mathbb{Z}$ lui-même.

- $\mathcal{P}(A)$ est un sous-anneau de $\mathcal{P}(E)$ si $A \subset E$.
- L'ensemble des fonctions constantes (resp. T-périodiques, continues, dérivables, bornées) constitue un sous-anneau de $\mathcal{F}(\mathbb{R}\,\mathbb{R})$.

REMARQUE 7.21 :

- *Un sous-anneau B d'un anneau A est lui-même un anneau : il peut être intègre alors que A ne l'est pas (les fonctions constantes parmi toutes les fonctions par exemple) mais le sous-anneau B est forcément intègre si l'anneau A l'est.*
- *On dispose comme pour les groupes de la notion d'***anneau produit** *de deux anneaux (on peut même généraliser à plusieurs anneaux) ; de plus, si A_1 et A_2 sont deux anneaux, on a : $(A_1 \times A_2)^\times = A_1^\times \times A_2^\times$.*
- *Une intersection de sous-anneaux est encore un sous-anneau ce qui nous permet d'affirmer que l'intersection de tous les sous-anneaux de A qui contiennent X (où $X \subset A$) est lui-même un sous-anneau qui contient X et c'est le plus petit de tous les sous-anneaux qui contiennent X ; cela nous donne la notion de sous-anneau engendré par une partie.*

Définition 7.22

Soit A et A' deux anneaux et $f : A \to A'$ une application, on dit que f est un **morphisme d'anneaux** *si les propriétés suivantes sont vérifiées :*

- *f est un morphisme de groupes.*
- $f(1_A) = 1_{A'}$.
- $\forall (x, y) \in A^2,\ f(xy) = f(x)f(y)$.

De plus, comme pour les groupes, f est appelé :

- *un* **isomorphisme d'anneaux** *si f est bijective.*
- *un* **endomorphisme d'anneaux** *si $A = A'$ (en tant qu'anneau).*
- *un* **automorphisme d'anneaux** *si $A = A'$ et f bijective.*

EXEMPLE 7.23 : • La conjugaison est un automorphisme d'anneaux dans $\mathbb{C}$.

- $\varphi : \mathcal{F}(\mathbb{R}, \mathbb{R}) \to \mathbb{R}$ définie par : $\forall f \in \mathcal{F}(\mathbb{R}, \mathbb{R}),\ \varphi(f) = f(0)$ est un morphisme d'anneaux.

Proposition 7.12

Si f est un morphisme d'anneaux, alors on a les propriétés suivantes :

- $f(0_A) = 0_{A'}$ **et** $f(1_A) = 1_{A'}$ **(on le savait déjà).**
- $\forall (x,y) \in A^2,\ f(x+y) = f(x) + f(y)$, $f(xy) = f(x)f(y)$, $f(-x) = -f(x)$ **(on le savait aussi).**
- **Si** $x \in A$**, on a en général :** $\forall n \in \mathbb{N},\ f(x^n) = f(x)^n$ **et** $\forall n \in \mathbb{Z},\ f(nx) = nf(x)$.
- **Si** x **est inversible dans** A **alors** $f(x)$ **est inversible dans** A' **et** $(f(x))^{-1} = f(x^{-1})$.
- **Si** x **est inversible dans** A **alors on a même :** $\forall n \in \mathbb{Z},\ f(x^n) = f(x)^n$.

Proposition 7.13

Si $f : A \to A'$ **et** $g : A' \to A''$ **sont deux morphismes d'anneaux alors** $g \circ f$ **est un morphisme d'anneaux. De plus, si** B **est un sous-anneau de** A **et** B' **un sous-anneau de** A' **alors** $\widehat{f}(B)$ **est un sous-anneau de** A' **et** $f^{<-1>}(B')$ **est un sous-anneau de** A.

REMARQUE 7.22 : Attention car $\mathrm{Im}(f) = \widehat{f}(A)$ *est bien un sous-anneau de* A' *si* $f : A \to A'$ *est un morphisme d'anneaux (car* A *est un sous-anneau de* A*) mais, par contre,* $\mathrm{Ker}(f) = f^{<-1>}(\{0_{A'}\})$ *n'est qu'un sous-groupe de* A *car* $\{0_{A'}\}$ *n'est qu'un sous-groupe de* A'*. Heureusement nous avons encore :*

Théorème 7.3

Si $f : A \to A'$ **est un morphisme d'anneaux alors :**

- f **est injective** $\iff \mathrm{Ker}(f) = \{0_A\}$.
- f **surjective** $\iff \mathrm{Im}(f) = A'$.

7.3.4 : La structure de corps

Définition 7.23

Soit K *un ensemble non vide muni de deux lois internes* $+$ *et* $\times$ *; on dit que* $(K, +, \times)$ *est un* **corps** *si* $(K, +, \times)$ *est un anneau et si tout élément de* K *est inversible (c'est-à-dire* $K^\times = K \setminus \{0_K\} = K^*$*). De plus, si la loi* $\times$ *est commutative, on dira que* K *est un* **corps commutatif**.

EXEMPLE 7.24 : • $\mathbb{Q}$, $\mathbb{R}$ et $\mathbb{C}$ sont des corps pour les lois $+$ et $\times$.
• $\mathbb{Z}/7\mathbb{Z}$ muni des lois $+$ et $\times$ modulo 7 est un corps commutatif.

REMARQUE 7.23 : Un corps est un anneau intègre mais un anneau intègre n'est pas forcément un corps.

Définition 7.24

Soit L *un corps et* $K \subset L$ *; on dit que* K *est un* **sous-corps** *de* L *si* K *est un sous-anneau de* L *et si tout élément non nul de* K *possède un inverse dans* K *; c'est-à-dire si* $\forall x \in K^*,\ x^{-1} \in K$.

EXEMPLE 7.25 : • $\mathbb{Q}$ est un sous-corps de $\mathbb{R}$ qui est lui-même un sous-corps de $\mathbb{C}$.
• $\mathbb{Q}(\sqrt{2}) = \{a + b\sqrt{2} \mid (a,b) \in \mathbb{Q}^2\}$ est un sous-corps de $\mathbb{R}$.

Définition 7.25

Soit K, K' *deux corps, alors* $f : K \to K'$ *est un* **morphisme de corps** *si c'est un morphisme d'anneaux.*

REMARQUE 7.24 : Il y a les mêmes définitions d'endomorphismes de corps, d'isomorphismes de corps et d'automorphismes de corps ; de plus nous avons des résultats similaires à ceux obtenus sur les groupes et les anneaux : la composée de deux morphismes en est un, l'image directe d'un sous-corps par un morphisme de corps est un sous-corps (même chose pour l'image réciproque) et on a encore la notion de sous-corps engendré par une partie.

EXEMPLE 7.26 : L'application $\varphi : \mathbb{Q}(\sqrt{2}) \to \mathbb{Q}(\sqrt{2})$ définie par $\varphi(a + b\sqrt{2}) = a - b\sqrt{2}$ pour tout couple $(a,b) \in \mathbb{Q}^2$ est un automorphisme de corps.